AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. **(Currently Amended)** A method of detecting critical file changes, comprising:

generating a read request for~~reading~~ an event representing at least one system call, wherein the event is a kernel audit record ~~read from~~ removed from a buffer of an intrusion detection data source (IDDS);

reading the requested event;

routing the event to a template, the event comprising multiple parameters and the template comprising a sequence of connected logic nodes comprising at least one input node, at least one filter node, and at least one output node;

filtering the event, based on the sequence of logic nodes of the template, as a possible intrusion based on the multiple parameters and either dropping the event or outputting the event, the filtering comprising:

determining a filename based on the event;

outputting the event for each event indicating modification of a critical file based upon the determined filename; and

creating an intrusion alert for each event output from said filtering.

2. (Previously Presented) The method of claim 1, wherein said filtering further comprises providing the event to the determining a filename for each event comprising a parameter indicating modification of a permission bit on a file or directory.

3. (Previously Presented) The method of claim 1, wherein said filtering further comprises providing the event to the determining a filename for each event comprising a parameter indicating opening a file for truncation.

4. (Previously Presented) The method of claim 1, wherein said filtering further comprises providing the event to the determining a filename for each event comprising a parameter indicating modification of the ownership or group ownership of a file.

5. (Previously Presented) The method of claim 1, further comprising an alert message for each renamed file including the filename of the file and the new filename of the renamed file.

6. (Previously Presented) The method of claim 1, comprising configuring a template based on a list of files and directories to be included or excluded based on whether the files and directories are considered unmodifiable.

7-12. (Cancelled)

13. (Previously Presented) A computer-readable medium storing instructions which, when executed by a processor, cause the processor to implement the method steps of claim 1.

14. **(Currently Amended)** A system for detecting critical file changes, comprising:

a processor; and

a memory storing instructions which, when executed by the processor, cause the processor to:

generate a read request for an event from an intrusion detection data source (IDDS), wherein the event is a kernel audit record removed from a buffer;

reading the requested event;

route events to a template, wherein the event comprises one or more parameters and the template comprises a sequence of connected logic nodes comprising at least one input node, at least one filter node, and at least one output node,

filter the event, based on the template, as a possible intrusion based on one of the one or more parameters and either dropping the event or outputting the event, and

create an intrusion alert for each event output from the filter.

15. (Previously Presented) The system of claim 20, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to provide the event to the determine a filename instructions for each event comprising one of the one or more parameters indicating modification of the permission bits on a file or directory.

16. (Previously Presented) The system of claim 20, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to provide the event to the determine a filename instructions for each event comprising one of the one or more parameters indicating that a file was opened for truncation.

17. (Previously Presented) The system of claim 20, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to provide the event to the determine a filename instructions for each event comprising one of the one or more parameters indicating modification of the ownership or group ownership of a file.

18. (Previously Presented) The system of claim 20, wherein the instructions further comprise instructions causing the processor to output an alert message for each renamed file, the alert message comprising the filename of the file and the filename of the renamed file.

19. (Previously Presented) The system of claim 20, wherein the instructions comprise instructions causing the processor to configure a template based on a list of files and directories to be included or excluded based on whether the files and directories are considered unmodifiable.

20. (Previously Presented) The system of claim 14, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to determine a filename based on the event and output the event for each event indicating modification of a critical file based upon the determined filename.

21. (Previously Presented) The method of claim 1, wherein said filtering further comprises determining a subdirectory of a directory based on the event and outputting the event for each event indicating modification to the determined subdirectory.

22. (Previously Presented) The system of claim 14, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to determine a subdirectory of a directory based on the event and output the event for each event indicating modification to a predetermined subdirectory of a directory.

23. (Previously Presented) The method of claim 1, wherein said reading an event comprises reading an event from an event-driven correlation service of the IDDS.

24. (Previously Presented) The system of claim 14, wherein the instructions causing the processor to read an event comprise instructions causing the processor to read an event from an event-driven correlation service of the IDDS.